Wojciech Danilczuk

Komputerowo wspomagane metody ilościowe w bezpieczeństwie maszyn

JEL: L62. DOI: 10.24136/atest.2018.007

Data zgłoszenia: 11.12.2017. Data akceptacji: 05.02.2018.

W artykule przedstawiono problematykę bezpieczeństwa maszyn w kontekście obowiązujących przepisów prawnych i norm międzynarodowych oraz komputerowo wspomagane metody przeprowadzania oceny zgodności i szacowania ryzyka. Na podstawie literatury oraz norm zostały za prezentowane najczęściej stosowane współczynniki oraz metody szacowania bezpieczeństwa. Następnie na przykładzie z praktyki przemysłowej autora została zaprezentowana metoda szacowania ryzyka z wykorzystaniem metod wspomaganých komputerowo. Do przeprowadzenia oceny zgodności autor wykorzystał oprogramowanie SISTEMA niemieckiego instytutu IFA [10]. Prezentowany przykład pokazuje możliwości zautomatyzowanie procedury obliczeniowej, przyspieszenia procesu oceny ryzyka oraz zmniejsza możliwość popełnienia błędu podczas projektowania układów związanych z bezpieczeństwem maszyn i urządzeń. Dodatkowym atutem metod komputerowych jest łatwość skalowania na większe i bardziej złożone układy.

Słowa kluczowe: ocena ryzyka, bezpieczeństwo maszyn, oprogramowanie SISTEMA.

Wstęp

Bezpieczeństwo maszyn jest jednym z kluczowych aspektów, jaki muszą brać pod uwagę inżynierowi zajmujący się projektowaniem i konstruowaniem nowych urządzeń. Zgodnie z dyrektywą maszynową i tzw. nowym podejściem producenci maszyn są zobowiązani do przeprowadzenia procedury oceny zgodności oraz oceny ryzyka [3]. Są to procedury niezbędne i wymagane do wystawienia deklaracji zgodności WE oraz znaku CE. Również polskie przepisy prawne [7] regulują wymagania dotyczące zasadniczych wymagań w zakresie bezpieczeństwa i ochrony zdrowia.

Z dyrektywa maszynową zharmonizowana jest norma PN-EN ISO 12100 [4] opisująca procedurę oceny ryzyka i metody zmniejszania ryzyka. Analiza ryzyka powinna być prowadzona już na etapie projektowania, czasem nawet na etapie koncepcji. Często wprowadzenie poprawek, nie tylko związanych z bezpieczeństwem, w momencie produkcji lub uruchamiania urządzenia jest bardzo kosztowna i pracochłonna. [9]. Procedury opisane w normie [4] mają charakter jakościowy. Metody i procedury ilościowe związane z bezpieczeństwem maszyn, wykorzystywane najczęściej w praktyce przemysłowej to określanie poziomu SIL zgodnie z normą PN-EN 62061 [6] oraz obliczanie poziomu PL na podstawie normy PN-EN ISO 13849 [5]. Wskaźnik SIL (ang. Safety integrity level, poziom nienaruszalności bezpieczeństwa) wykorzystywany jest przede wszystkim dla układów elektrycznych i elektronicznych (w tym programowalnych). Poziom

PL (ang. Performance level, poziom zapewnienia bezpieczeństwa) ma szersze zastosowanie, obejmuje on bowiem zarówno układy elektryczne jak i pneumatyczne, hydrauliczne i mechaniczne [9]. W dalszej części pracy autor skupi się na metodzie wyznaczania poziomu Performance Level. Osoby zainteresowane metodą SIL odsyłam do normy [6] oraz do licznych pozycji literatury zarówno akademickiej np. [2] jak i branżowej [8].

1. Algorytm wyznaczania PL według normy EN ISO 13849

1.1. Określenie PLr

Pierwszym etapem określenia poziomu zapewnienia nienaruszalności jest określenie wymaganego Poziomu Zapewnienie Bezpieczeństwa – PLr (ang. Performance level required). W tym celu należy posłużyć się grafem oceny ryzyka (rys. 1). Graf określa poziom PLr na podstawie kombinacji 3 predyktorów.

♦ S – ciężkość urazów

Urazy dzielimy na lekkie, odwracalne (S1) takie jak lekkie urazy, zranienie, otarcia oraz na ciężkie (S2), nieodwracalne. Zaliczamy do nich amputacje, śmierć i urazy powodujące trwałe kalectwo.

♦ F – częstość narażenia lub czas ekspozycji zagrożenia

W przypadku współczynnika F należy zwrócić szczególną uwagę na jego dwójaki charakter. Częstość narażenia jest wskaźnikiem intuicyjnym np. prasa hydrauliczna będzie miała częstotliwość narażenia operatora na niebezpieczeństwo zmiążdżenia wynikającą z cyklu produkcyjnego. Czas ekspozycji na zagrożenie nie powi-

Rys. 1. Graf oceny ryzyka: S – ciężar obrażeń, S1 – lekkie (odwracalne), S2 – ciężkie nieodwracalne/śmierć, F – czas i/lub częstotliwość narażenia na niebezpieczeństwo, F1 – rzdko lub średnio, F2 – często lub ciągle, P – możliwość zapobiegania zagrożeniom lub ograniczeniu szkód, P1 – możliwe w określonych warunkach, P2 – prawie niemożliwe [1]

nien być mylony z częstością użytkowania urządzenia np. szlifierka kontowa może być używana bardzo rzadko (raz w miesiącu przez godzinę) jednak czas ekspozycji na zagrożenie jest bardzo duży (przez godzinę użytkowania szlifierki jesteśmy narażeni na niebezpieczeństwo wynikające z wirującej tarczy). Współczynnik F również ma 2 poziomy. F1 – częstość narażenia jest rzadkie do dość częstego lub czas ekspozycji krótki. F2 – częste lub ciągle narażenie na ryzyko lub długi czas ekspozycji.

♦ P – możliwość uniknięcia zagrożenia

Określa możliwość uniknięcia zagrożenia w szczególnych warunkach (P1) – dobra widoczność, praca zgodnie z instrukcją obsługi i BPH, niskie prędkości. Dla przypadków gdzie uniknięcie zagrożenia jest niemożliwie lub prawie niemożliwe przyjmuje wartość P2.

1.2. Określenie architektury układu

Architektura układu zwana też strukturą może zostać podzielona na podstawowe komponenty. Każdy z tych komponentów pełni jedną z 3 funkcji: wejście do układu, logikę oraz wyjście z układu. Rozważmy przykład wyłącznika awaryjnego. Funkcje wejścia pełni przycisk E-Stop, logika układu może być sterownik bezpieczeństwa a wyjściem układu stycznik bezpieczeństwa. Architektura układu zależy min. od ilości kanałów (redundancji układu), zastosowania funkcji kontrolnych, odporności na uszkodzenie czy pokrycia diagnostycznego. Szczegóły znajdują się w tab 1.

1.3. Średni czas do niebezpiecznego uszkodzenia

Parametr MTTFd (ang. *Mean Time to Dangerous Failure*) – średni czas niebezpiecznego uszkodzenia (1), wyrażany jest w latach. Może być szacowany na podstawie metod dobrych praktyk inżynierskich (ang. *Good engineering practice method*), odczytany z dokumentacji elementu lub obliczany. MTTF_d oblicza się na podstawie wartości B_{10d} (określającą liczbę cykli, po którym niebezpiecznemu uszkodzeniu ulegnie 10% badanej populacji) oraz średniej liczby cykli na rok n_{op} (2)

$$MTTFd = \frac{B_{10d}}{0,1 \cdot n_{op}} \quad (1)$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 \text{ s/h}}{t_{cycle}} \quad (2)$$

gdzie:

d_{op} – średni czas pracy w dniach na rok;

h_{op} – średni czas pracy w godzinach na dzień;

t_{cycle} – średni czas między rozpoczęciem dwóch kolejnych cykli.

Na podstawie wartości B_{10d} oraz n_{op} możemy obliczyć również średni czas do niebezpiecznego uszkodzenia 10% elementów – T_{10d} (3). Czas ten (wyrażony w latach) powinien zostać porównany z założonym czasem użytkowania urządzenia (ang. *Mission time*).

$$T_{10d} = \frac{B_{10d}}{n_{op}} \quad (3)$$

Średni czas niebezpiecznego uszkodzenia jest klasyfikowany do jednego z 3 zakresów (krótki, średni i długi) – tab. 2.

1.4. Pokrycie diagnostyczne

Pokrycie diagnostyczne DC (ang. *Diagnostic Coverage*) oblicza się ze wzoru (4). Często praktyką jest odszukiwanie wartości DC bezpośrednio z normy [5]. Po obliczeniu wartości pokrycia diagnostycznego, podobnie jak w przypadku MTTFd klasyfikuje się je do jednej kategorii (tab. 3).

$$DC = \frac{\Sigma \lambda_{dd}}{\Sigma \lambda_{dd} + \Sigma \lambda_{du}} \quad (4)$$

gdzie:

λ_{dd} – intensywność wykrywalnych niebezpiecznych uszkodzeń [1/h];

λ_{du} – intensywność niewykrywalnych niebezpiecznych uszkodzeń [1/h].

Tab. 2. Zakresy MTTFd [9]

OZNACZENIE	ZAKRES DLA KANAŁU
Krótki	3 lata ≤ MTTFd < 10 lat
Średni	10 lat ≤ MTTFd < 30 lat
Długi	30 lat ≤ MTTFd ≤ 100 lat

Tab. 3. Zakres DC [9]

BRAK	< 60 %
NISKIE	60 % ≤ DC < 90 %
ŚREDNIE	90 % ≤ DC < 99 %
WYSOKIE	DC ≥ 99 %

Tab. 1. Podział architektury podsystemów [9]

KATEGORIA	CHARAKTERYSTYKA
B	Zastosowanie elementów zgodnych z normami i podstawowymi zasadami bezpieczeństwa, wytrzymujące przewidywane narażenia. Wystąpienie uszkodzenia może powodować utratę funkcji bezpieczeństwa.
1	Jak w B oraz zastosowano wypróbowane elementy i sprawdzone zasady bezpieczeństwa. Wystąpienie uszkodzenia może powodować utratę funkcji bezpieczeństwa, ale prawdopodobieństwo tego jest niższe niż w kategorii B.
2	Jak w B oraz zastosowano sprawdzone zasady bezpieczeństwa. Funkcja bezpieczeństwa jest sprawdzana przez układ sterowania. Wystąpienie uszkodzenia może powodować utratę funkcji bezpieczeństwa między sprawdzeniami.
3	Jak w B oraz zastosowano sprawdzone zasady bezpieczeństwa. Struktura odporna na uszkodzenie. Uszkodzenia są wykrywane (małe i średnie pokrycie diagnostyczne).
4	Jak w B oraz zastosowano sprawdzone zasady bezpieczeństwa. Struktura odporna na uszkodzenie. Wysokie pokrycie diagnostyczne. Wykrywanie uszkodzeń zapobiega utracie bezpieczeństwa.

Tab. 4. Określenie poziomu CCF [9]

ŚRODEK/WYMAGANIE		PUNKTY
Odseparowanie	Odseparowanie obwodów sygnałowych (przewodów elektrycznych, hydraulicznych, cięgien mechanicznych), dostateczne odstępy powierzchniowe i powietrzne.	15
Zróżnicowanie	Różne technologie lub fizyczne zasady, np. – pierwszy kanał programowalny a drugi kanał sprzętowy, – pomiar cyfrowy i analogowy; elementy różnych producentów.	20
Projekt, doświadczenie	Ochrona przed przepięciem, przeciążeniem, zwiększonym ciśnieniem, np. w mechanice sprzęgła przeciążeniowe.	15
	Zastosowanie wypróbowanych elementów.	5
Analiza	Przeprowadzenie analizy rodzajów i skutków uszkodzeń (FMEA), aby uniknąć uszkodzeń spowodowanych wspólną przyczyną w projektowaniu.	5
Szkolenia	Szkolenie projektantów w kierunku pojmowania przyczyn i skutków uszkodzeń spowodowanych wspólną przyczyną.	5
Wpływy środowiska	Badania na kompatybilność elektromagnetyczną.	25
	Testy systemu pod kątem wpływu temperatury, wstrząsów, wibracji, wilgotności, substancji korozyjnych itp.	10

Tab. 5. Określenie poziomu PL [9]

KATEGORIA	B	1	2	2	3	3	4
DC	Brak	Brak	Niskie	Średnie	Niskie	Średnie	Wysokie
MTTFd							
Krótki	PL a	–	PL a	PL b	PL b	PL c	–
Średni	PL b	–	PL b	PL c	PL c	PL d	–
Długi	–	PL c	PL c	PL d	PL d	PL d	PL e

1.5. Odporność na uszkodzenie spowodowane wspólną przyczyną

Ostatnim współczynnikiem który należy obliczyć w celu określenia poziomu PL systemu jest odporność na uszkodzenie spowodowane wspólną przyczyną CCF (ang. *Common Cause Failure*). Analizując środki i wymagania chroniące przed uszkodzeniem przynajmniej się maksymalną liczbę punktów dla danego środka lub zero (tab. 4). Maksymalna liczba punktów jaką można uzyskać to 100, natomiast wymagane jest co najmniej 65. Sprawdzenie odporności CCF wymagane jest tylko dla kategorii 2, 3 i 4.

1.6. Określenie poziomu PL

Po obliczeniu parametrów PL_r, MTTF_d, DC i CCF możemy określić PL naszego systemu (tab. 5). Jeśli jest on nie mniejszy od wymaganego PL_r to stwierdza się, że układ jest bezpieczny i spełnia wymagania.

2. Oprogramowanie SISTEMA

Program SISTEMA zalicza się do programów CAE (ang. *Computer Aided Engineering*). Został opracowany przez niemiecki instytut IFA (de. *Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung*) specjalizujący się w badaniach nad bezpieczeństwem pracy [10]. Służy on do komputerowo wspomaganego określania poziomu bezpieczeństwa maszyn zgodnie z wymogami normy [5]. Co nie często spotykane jest on programem darmowym z możliwością wykorzystania komercyjnego, naukowego i prywatnego. Wielu producentów mających w swej ofercie komponenty związane z bezpieczeństwem maszyn udostępnia darmowe biblioteki elementów kompatybilne z oprogramowaniem SISTEMA (min. Schneider Electric, Pilz, Rockwell Automation).

Użycie bibliotek gotowych elementów oraz możliwość automatycznego obliczenia wszystkich parametrów związanych z poziomem bezpieczeństwa maszyn ułatwia prace osobom projektującym maszyn wyposażone w elementy bezpieczeństwa. Zmniejsza

się też ryzyko popełnienia błędu w określaniu poziomu zapewnienia bezpieczeństwa zwłaszcza dla bardziej rozbudowanych skomplikowanych urządzeń.

3. Przykład wykorzystania komputerowo wspomaganego systemu do oceny bezpieczeństwa urządzenia

Użycie programu SISTEMA do określenia poziomu PL urządzenia zostanie zaprezentowane na przykładzie z praktyki zawodowej autora. Analizowane urządzenie to dedykowany stół montażowy. Instalacja detalu na stole odbywa się z użyciem wózka paletowego. Po przytwierdzeniu detalu operator ma możliwość podniesienia powierzchni roboczej na pożądaną wysokość (urządzenie wykorzystuje do tego siłownik hydrauliczny). Po zakończonej pracy z półfabrykatem operator opuszcza stół i detale jest przekazywany na dalsze stanowiska.

Jednym z niebezpieczeństw wynikających z pracy z urządzeniem jest ruch kolumn nośnych na których znajduje się blat montażowy. Jako funkcje bezpieczeństwa zdefiniowano zatrzymanie ruchu kolumn nośnych po wciśnięciu przycisku E-STOP. Do realizacji tej funkcji niezbędne były 2 elementy – przycisk awaryjnego zatrzymania E-STOP (wejście systemu), przekaźnik bezpieczeństwa z funkcją stykownika bezpieczeństwa (logika systemu). Po wciśnięciu przycisku E-STOP przekaźnik odcinał zasilanie w obwodzie sterującym ruchem kolumn, elektrozawór 5/3 sterujący ruchem kolumn wraca do pozycji środkowej i następuje zatrzymanie. Elementem wykonawczym jaki również wziąć pod uwagę analizując bezpieczeństwo urządzenia jest elektrozawór sterujący ruchem kolumn (wyjście układu).

Schemat sterowania obwodem bezpieczeństwa przedstawia rys 2.

Analiza układu bezpieczeństwa w programie SISTEMA przebiega zgodnie z normą [5]. W pierwszej kolejności należy określić PL_r (rys. 3). Dla rozważanego przykładu określono ciężkość urazów

Rys. 2. Schemat sterowania obwodem bezpieczeństwa

Źródło: oprac. własne.

Rys. 3. Wymagany PLr

Źródło: oprac. własne.

Rys. 4. Obliczenie MTTFd w programie SISTEMA

Źródło: oprac. własne.

S2 (urazy ciężkie) – podnoszony detal ma dużą masę i możliwe jest niebezpieczne zmiążdżenie. Częstość narażenia na niebezpieczeństwo określono jako F1 (niewielkie) – ruch kolumn ma charakter ruchu pomocniczego w procesie. Niebezpieczeństwo uznano za możliwe do zminimalizowania z zachowaniem środków ostrożności P1 – przeszkolenie osób pracujących z urządzeniem, piktogramy ostrzegawcze. Wymagany poziom PLr wyniósł C. Następnie należało dodać komponenty realizujące poszczególne funkcje. Przycisk E-STOP oraz przełącznik bezpieczeństwa zostały zaimportowane z bibliotek producentów. Elektrozawór 5/3 sterujący ruchem kolumn został określony jako element o kategorii 1 (element ten jest zgodny z normami, wykorzystanie go jako zabezpieczenie ruchu siłownika hydraulicznego jest zgodne z wypróbowanymi zasadami bezpieczeństwa). Następnie obliczono MTTDd zaworu. Ze względu na brak danych o wartości B_{10d} przyjęto wartość zgodną z dobrymi praktykami inżynierskimi $B_{10d} = 20\,000\,000$. Średniej liczby cykli na rok n_{op} została określona na 3 750 (praca przez 250 dni w roku, średnio 15 godz. dziennie, szacowany czas między kolejnymi podnoszeniem i opuszczeniem kolumn to 1 godz.). Wartość $MTTF_d$ została określona na 53 333,33 (rys. 4).

Uzyskany poziom PL rozpatrywanej funkcji bezpieczeństwa wyniósł C i jest on nie mniejszy niż wymagane PLr. Rozwiązanie zostało uznane za bezpieczne.

Podsumowanie

Znajomość przepisów i norm dotyczących bezpieczeństwa maszyn jest jednym z podstawowych kompetencji inżynierów zajmujących się konstrukcją urządzeń. Wykorzystanie metod komputerowych do oceny bezpieczeństwa powinno być w ocenie autora powszechną praktyką. Ocena ryzyka jest jedną z podstawowych analiz jakim powinno się poddawać każde projektowane urządzenie. Wykorzystanie specjalistycznego oprogramowania jak opisana w artykule SISTEMA usprawnia proces projektowania i walidacji układów bezpieczeństwa. Zmniejsza również ryzyko popełnienia błędów, zwłaszcza przy analizie bardziej złożonych układów.

Osobom zainteresowanym praktycznym wykorzystaniem normy [5] oraz poszerzenia swojej wiedzy z zakresu oprogramowania SISTEMA autor szczególnie poleca pozycję [8].

Bibliografia:

1. Łabanowski W., *Bezpieczeństwo użytkowania maszyn*, Państwowa Inspekcja Pracy, Główny Inspektorat Pracy, Warszawa 2013.
2. Marszał E. M., Scharpf E. W., *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis*, Instrumentation, Systems, and Automation Society, 2002.
3. Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE.
4. Norma PN-EN ISO 12100: Bezpieczeństwo maszyn. Ogólne zasady projektowania. Ocena ryzyka i zmniejszanie ryzyka.
5. Norma PN-EN ISO 13849 1:2008: Bezpieczeństwo maszyn. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania.
6. Norma PN-EN ISO 62061:2008: Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
7. Rozporządzenie Ministra Gospodarki z dnia 21 października 2008 r. w sprawie zasadniczych wymagań dla maszyn (Dz. U 2008, nr 199, poz. 1228).
8. Podręcznik Bezpieczeństwa Maszyn 5. Poradnik bezpieczeństwa maszyn – przepisy prawne, teoria i praktyka. Rockwell Automation.
9. Kasprzyczak L., Wyznaczanie poziomów bezpieczeństwa SIL i PL, „Automatyka” 2015, 1–2.
10. The official home of the IFA Institute 2018: <http://www.dguv.de>
11. Łygas K., Danilczuk W., *Translator G-codu na język robota Kawasaki*, „Autobusy – Technika, Eksploatacja, Systemy Transportowe” 2017, nr 6.
12. Łygas K., Danilczuk W., *Stanowisko do aplikacji pick’n’place z wykorzystaniem systemu wizyjnego i autorskiego interfejsu komunikacji*, „Autobusy – Technika, Eksploatacja, Systemy Transportowe” 2017, nr 6.

Autor:

mgr inż. **Wojciech Danilczuk** – Politechnika Lubelska, Wydział Mechaniczny, Katedra Automatykacji

Computer aided quantitative methods in machine safety

The paper present aspect of machine safety in addition to current legal regulations and international standards and computer aided method of risk analysis. Based on literate and international standards paper author presents most common factors and method of safety estimation. Next, based on author industry experience, computer aided risk analysis has been present. To proceed conformity assessment author used SISTEMA software developed by German institute IFA [10]. The example shown shows simplify calculation method of risk analysis and decrees level of mistake during to designee of machine safety component. Another advantages of computer aided method is simplify to scale it to the more complex system.

Keywords: risk assessment, machine safety, SISTEMA software.